EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 09212365
PUBLICATION DATE : 15-08-97

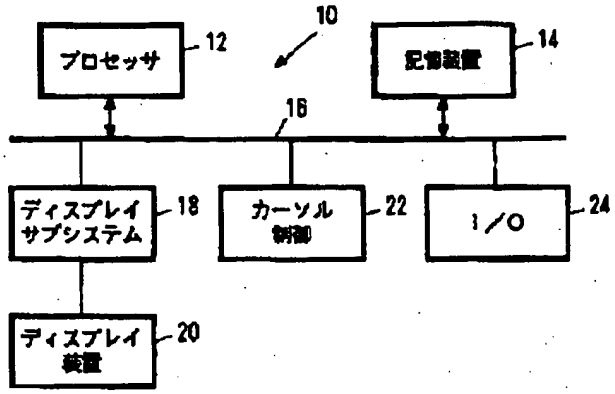
APPLICATION DATE : 25-12-96
APPLICATION NUMBER : 08345679

APPLICANT : INTERNATL BUSINESS MACH CORP <IBM>;

INVENTOR : NADALIN ANTHONY J;

INT.CL. : G06F 9/44 G06F 12/14

TITLE : SYSTEM, METHOD, AND PRODUCT FOR INFORMATION HANDLING INCLUDING INTEGRATION OF OBJECT SECURITY SERVICE APPROVAL IN DECENTRALIZED COMPUTING ENVIRONMENT



ABSTRACT : PROBLEM TO BE SOLVED: To integrate object security service approvals in a decentralized computing environment by allocating and selecting a set of method request access rights.

SOLUTION: The information handling system 10 is equipped with a processor 12, a storage device 14, a system bus 16, a display subsystem 18 which controls a display device 20, a cursor controller 22, and an I/O controller 24. An object- oriented control program maps a set of methods defined in a given class to a set of fixed finite access rights to which a set of method request access rights is assigned. And, a set of permissions regarding a 1st and a 2nd family right type permissions is inspected to select a set of access rights.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－212365

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/44	５３０		Ｇ０６Ｆ	9/44	５３０Ｃ
	12/14	３１０			12/14	３１０Ｋ

審査請求　未請求　請求項の数14　ＯＬ　（全７頁）

(21)出願番号　特願平8－345679

(22)出願日　平成８年(1996)12月25日

(31)優先権主張番号　０８／５８２５５０

(32)優先日　1996年１月３日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　メサウド・ベナンタール
アメリカ合衆国12603、　ニューヨーク州　ポウキプスィ　ジャックマン　ドライブ　エス　39－ビー

(74)代理人　弁理士　合田　潔　（外２名）

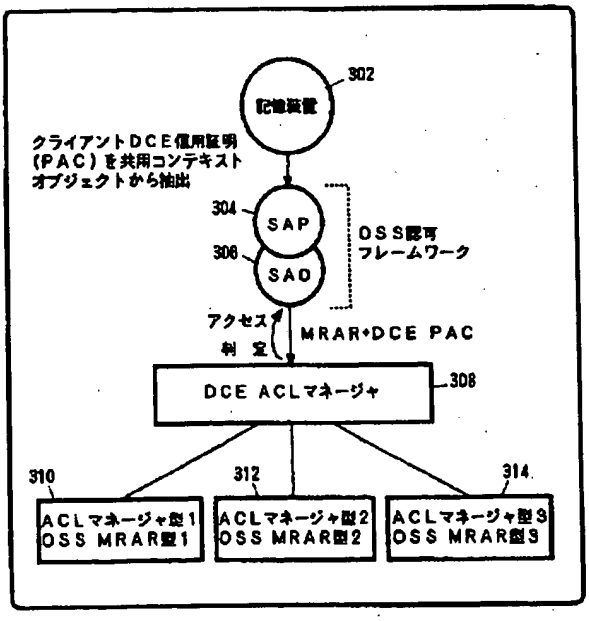
最終頁に続く

(54)【発明の名称】　分散コンピューティング環境でのオブジェクト・セキュリティ・サービス認可の統合を含む情報取り扱いシステム、方法および製品

(57)【要約】

【課題】分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合する。

【解決手段】オブジェクト指向制御プログラムが、所与のクラスによって定義されるメソッドのセットを、メソッド要求アクセス権のセットが割り当てられる固定された有限のアクセス権のセットに対してマッピングすることと、二つの要素、すなわち第一のファミリー権利型（権利型とは、その許可のセットの意味規則を指図する要素である）および第二の、そのようなファミリーそれぞれに関する許可のセットを検査することによってアクセス権のセットを選択することとを含む。二つのファミリー型、すなわちオペレーション権利および役割権利を用いることができる。本発明の実施態様のスケーリング性は、新たな権利型のファミリーを、ファミリーごとに対応する許可のセットとともに追加する能力によって実証することができる。



【特許請求の範囲】
【請求項１】第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするステップと、
メソッド要求アクセス権のセットを割り当てるステップと、
前記アクセス権のセットを選択するステップと、を含むことを特徴とする、情報取り扱いシステムにおいてオブジェクト指向技術を用いる方法。
【請求項２】前記方法かステップが、
前記アクセス権のセットの二つの要素を検査するステップをさらに含む請求項１記載の方法。
【請求項３】前記二つの要素の第一のものがファミリー権利型である請求項１記載の方法。
【請求項４】前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである請求項１記載の方法。
【請求項５】ファミリー権利型が、
オペレーション権利と、
役割権利と、を含む請求項３記載の方法。
【請求項６】第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、
メソッド要求アクセス権のセットを割り当てるための手段と、
前記アクセス権のセットを選択するための手段と、をさらに含むコンピュータ読み出し可能媒体。
【請求項７】前記媒体が、前記アクセス権のセットの二つの要素を検査するための手段をさらに含む請求項６記載のコンピュータ読み出し可能媒体。
【請求項８】前記二つの要素の第一のものがファミリー権利型であり、
前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである請求項５記載のコンピュータ読み出し可能媒体。
【請求項９】１個以上のプロセッサと、
記憶装置と、
ディスプレイ装置を制御するディスプレイ・サブシステムと、
カーソル制御装置と、
１個以上のＩ／Ｏ装置を制御する１個以上のＩ／Ｏ制御装置と、
前記プロセッサ、前記記憶装置、前記ディスプレイ・サブシステム、前記カーソル制御装置および前記Ｉ／Ｏ制御装置を接続するシステム・バスと、
システムの動作を制御するためのオペレーティング・システム・プログラムと、
ユーザ・タスクを実行するための一つ以上のアプリケーション・プログラムと、
オブジェクト指向制御プログラムと、を含み、
前記オブジェクト指向制御プログラムが、
第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、
メソッド要求アクセス権のセットを割り当てるための手段と、
前記アクセス権のセットを選択するための手段と、を含むことを特徴とする、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合するための情報取り扱いシステム。
【請求項１０】前記アクセス権のセットの二つの要素を検査するための手段をさらに含む請求項９記載の情報取り扱いシステム。
【請求項１１】前記二つの要素の第一のものがファミリー権利型である請求項１０記載の情報取り扱いシステム。
【請求項１２】前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである請求項１０記載の情報取り扱いシステム。
【請求項１３】前記ファミリー権利型が、関連する許可のセットの意味規則を制御する要素である請求項１１記載の情報取り扱いシステム。
【請求項１４】ファミリー権利型が、
オペレーション権利と、
役割権利と、を含む請求項１０記載の情報取り扱いシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報取り扱いシステム、方法および製品に関し、より詳細には、オブジェクト指向システムにおいてオブジェクト・セキュリティを高めるための情報取り扱いシステム、方法および製品に関する。
【０００２】
【従来の技術】オブジェクト指向システムにおいてはセキュリティを改善する必要がある。従来から、リソースへのアクセスを制御することは、データを開示したり、変更したり、更新したりすることができるかどうかを決定することを意味する。しかし、オブジェクト指向システムにおけるアクセス制御は、異なるアスペクトおよび意味規則を呈する。オブジェクト指向システムにおいては、リソースは、データのみからなるオブジェクトではなく、オブジェクトのデータを改ざん、変形することができる操作をも含むオブジェクトである。そのようなものとして、オブジェクト・アクセス制御は、どのユーザがどのオブジェクトに対してどのメソッドを呼び出すことができるかの決定に関する。したがって、アクセス権が、それが当てはまるメソッドの機能性および副作用の意味規則に対応しなければならない。もっとも簡単な場合、この対応は１対１であることができる。すなわち、

メソッドMの必要なアクセス権は、そのメソッドの名称、すなわち単にMによってそれを定義するクラスにおいて一意的に識別することができる。したがって、主体は、メソッドMを呼び出し、その副作用を期待するためには、許可Mを取得しなければならないであろう。しかし、オブジェクト指向システムは、それぞれ異なるシグナチャおよび意味規則をもつ非常に多数のタイプのオペレーション（メソッド）を露呈する傾向にあるため、この方法は、スケールの問題を招く。アプリケーションの保護されたオブジェクトに対するこのようなアクセス制御は、アクセス権または許可の意味規則が一般に手近にあるアプリケーションだけに有効であるということにおいて、その特定のアプリケーションに適合させなければならない。加えて、クラス・ライブラリが新たに導入されるごとにアクセス権または許可のセットがサイズを急速に増すため、オブジェクト・アクセス制御の管理は複雑なタスクになる。

【０００３】従来技術において、オブジェクト指向プログラミング・システム（ＯＯＰＳ）を改善するための技術が数多くある。

【０００４】以下に従来技術の例を示す。

【０００５】米国特許第４，５２５，７８０号明細書は、オブジェクトに編成されたメモリを有するデータ処理システムであって、システムが、ユーザを識別する主体番号、ユーザの手続きを実行するためのプロセスおよびユーザの手続きによって実行されるシステム・オペレーションのタイプによって識別されるユーザによるオブジェクトに対する無許可のアクセスを防止する保護技術を利用するシステムを教示している。

【０００６】米国特許第５，１３６，７１２号明細書は、オブジェクトをプロセスに対して私用にするための手段を含む、マルチタスク処理コンピュータ・システムに用いるためのオブジェクトベースのオペレーティング・システムを教示している。私用オブジェクトに対するアクセスは、アクセス制御リストによって制御される。

【０００７】米国特許第５，２６５，２２１号明細書は、動詞、パラメータ、属性および機能のシステムを使用して、オブジェクトに対する認可を付与し、取り消し、否定するためのアクセス制御機構を教示している。

【０００８】米国特許第５，２９７，２８３号明細書および米国特許第５，３２１，８４１号明細書は、上記に論じた米国特許第５，１３６，７１２号明細書と同じシステムを教示していると思われる。

【０００９】米国特許第５，０９３，９１４号明細書は、概して、オブジェクト指向プログラムの実行の制御において、定義された動作を実施する、例えば、プログラムの実行中に指定のオブジェクトに対して指定の仮想機能が呼びされたときにプログラムを停止するために、デジタル・コンピュータによって使用される方法を教示している。

【００１０】米国特許第５，３４３，５５４号明細書は、第二のクラス・オブジェクトが外部的に呼び出し可能であり、外部的に呼び出し可能であるサブクラス・オブジェクトが内部的に呼び出し可能なサブクラス・オブジェクトの指示を含むような第一および第二のクラスのオブジェクトを作成することと、一つの外部的に呼び出し可能なサブオブジェクトが内部的に呼び出し可能なサブオブジェクトを呼び出し、その結果に応じて第一のクラスの新たなオブジェクトが生成されるようなオブジェクトのクラスを実行することとを含むプロセスによって問題が解決されるコンピューティング・システムを教示している。

【００１１】これらの特許は、一般に、オブジェクト指向プログラムにおいてオブジェクトをアクセスから保護する方法を扱うが、これらは、本明細書の特許請求の範囲の記載の開示するような、メソッド要求アクセス権のセットを割り当て、選択することによってスケールの問題を解決することを教示してもいないし示唆してもいない。

【００１２】オブジェクト・サービス機能、例えば持続性、回復性、並行性およびセキュリティを自動的に２進（バイナリ）クラスに追加する必要がある。ときには、クラスのソース・コードを変更できないこともある。ソース・コードを変更することができる場合でさえ、オブジェクト・サービス機能を追加するためには相当な再プログラムの努力を要する。

【００１３】

【発明が解決しようとする課題】本発明の目的は、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合することにある。

【００１４】

【課題を解決するための手段】したがって、分散コンピューティング環境においてオブジェクト・セキュリティサービス認可を統合するためのシステム、方法および製品は、１個以上のプロセッサと、記憶装置と、システム・バスと、ディスプレイ装置を制御するディスプレイ・サブシステムと、カーソル制御装置と、Ｉ／Ｏ装置を制御するＩ／Ｏ制御装置と（すべてシステム・バスによって接続）、オペレーティング・システム、例えばＯＳ／２オペレーティング・システム・プログラム（ＯＳ／２はInternational Business Machines社の登録商標である）と、ユーザ・タスクを実行するための一つ以上のアプリケーション・プログラムと、オブジェクト指向制御プログラム、例えば、International Business Machines社の市販品であるＤＳＯＭオブジェクト・プログラムとを含み、前記オブジェクト指向制御プログラムが、所与のクラスによって定義されるメソッドのセットを、メソッド要求アクセス権のセットが割り当てられる固定された有限のアクセス権のセットに対してマッピングすることと、二つの要素、すなわち第一のファミリー権利型

（権利型とは、その許可のセットの意味規則を指図する要素である）および第二の、そのようなファミリーそれぞれに関する許可のセットを検査することによってアクセス権のセットを選択することとを含む。二つのファミリー型、すなわちオペレーション権利および役割権利を用いることができる。本発明の実施態様のスケーラビリティ（拡張性）は、新たな権利型のファミリーを、ファミリーごとに対応する許可のセットとともに追加する能力によって実証することができる。

【００１５】本発明の利点は、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合することにより、分散オブジェクト・システムにおけるオブジェクト・セキュリティが改善されることにある。

【００１６】

【発明の実施の形態】まず、図１および２を参照しながら、本発明の情報取り扱いシステム１０およびオペレーティング・システム環境を説明する。

【００１７】情報取り扱いシステム１０は、１個以上のプロセッサ１２、記憶装置１４、システム・バス１６、ディスプレイ装置２０を制御するディスプレイ・サブシステム１８、カーソル制御装置２２および１／Ｏ制御装置２４（すべてシステム・バス１６によって接続）を備えたグラフィックス・ワークステーションなどであることができる。図１に示す情報取り扱いシステム１０は、市販されている周知のマルチタスク処理オペレーティング・システム、例えばＯＳ／２（ＯＳ／２はInternational Business Machines社の登録商標である）によって動作することができる。情報取り扱いシステム１０を動作させる際にＯＳ／２オペレーティング・システムが制御する多数のタスクの中には、オブジェクト指向プログラム、例えば、International Business Machines社の市販品であるＤＳＯＭオブジェクト・プログラムの実行がある。

【００１８】本発明の方法は、ＤＳＯＭオブジェクト・プログラムに組み入れることができる。

【００１９】２進クラスのオブジェクトのアクセス制御はオブジェクト保証（Secure object）サービスによって提供される。このオブジェクト保証サービスを説明する。

【００２０】ユーザがセキュリティを指定する方法は、クラス・オブジェクトを探索するときに、以下の制約を指定することである。

【００２１】名称：保証
値：オブジェクトがアクセス制御検査によって保護されるかどうかを示す論理フラグ
名称：ＡＣＬ
値：保証＝真ならば、アクセス制御リスト

【００２２】実現方法がメソッドによるとき、メソッドの呼び出しに応じて実施することができるか、参照が最初に得られたときに実施することができるかのいずれかである（ケイパビリティ方式）。ケイパビリティ（資格）方式は、オブジェクトと、許可されたメソッドのサブセットだけを有するＡＣＬ（許可されたメソッドのリスト）との組み合わせごとにセキュリティ代理（proxy）オブジェクトをサーバ中に構築することによって実施することができる。これを実施するためには、ＯＲＢ（または少なくともサーバ・オブジェクト）を変更しなければならないであろう。

【００２３】リソースに対するアクセスを制御する際には、アクセス権または許可のセットが、それらが当てはまるメソッドの意味規則に対応しなければならない。新たなクラス・ライブラリが導入されるごとにアクセス権または許可のセットがサイズを増すため、オブジェクト・アクセス制御の管理は複雑なタスクになる。スケーリング性を扱うためには、所与のクラスによって定義されるメソッドのセットを、メソッド要求アクセス権のセット（ＭＲＡＲ）が割り当てられる固定された有限のアクセス権のセットに対してマッピングする。そして、問題は、適当なアクセス権のセットを選択するということになる。セットを二つの要素、すなわち、ファミリー権利型と、そのようなファリミーそれぞれに関する許可のセットとに分割することにより、多数のアクセス権または許可のセットを有するシステムにおいてさえ、アクセス制御を効率的に扱うことができる。

【００２４】本発明の好ましい実施態様においては、二つの標準的なファミリー型、すなわちオペレーション権利および役割権利を述べる。スケーリング性の課題は、システムが新たな権利型のファミリーを、そのようなファミリーごとに対応する許可のセットとともに追加する能力によって取り扱われる。好ましくは標準タイプのオペレーション型および役割型に限定された少数のファミリー権利型を各ファミリー内の固定された少数の許可のセットとともに維持するならば、アクセス制御および移植性が高まる。

【００２５】以下の表１は、二つの標準的な権利型をその関連の権利および解釈とともに示す。

【００２６】

【表１】

表Ｉ

権利型		
権　利		意図する解釈
	R	読み
	W	書き

権利型
OPERATION_RIGHTS

ROLE_RIGHTS

X　実行
C　制御
D　削除
A　追加
G　ゲスト
U　ユーザ
O　オペレータ
M　管理者
T　監査者
S　監督者

【００２７】次に図３を参照しながら、本発明と、分散コンピューティング環境の認可機構との統合を説明する。セキュリティ記憶装置（vault）３０２がオブジェクト・セキュリティ・サービスの基本要素である。認可信用証明（credential）がオブジェクトごとに記憶装置３０２中に記憶されている。クライアントのＤＣＥ信用証明が共有コンテキスト・オブジェクトから抽出され、システム認可方針オブジェクト３０４に提示され、このシステム認可方針オブジェクトが、システム認可オラクル（oracle）３０６と合わさって、事前に確立した認可方針に基づき、認可の判定を下す。認可の判定は、システム認可オラクル３０６からＤＣＥ　ＡＣＬマネージャ３０８に送られる。メソッドのＭＲＡＲ権利型は、ＤＣＥ　ＡＣＬマネージャの型、例えばＡＣＬマネージャ型１およびＭＲＡＲ型１（３１０）、ＡＣＬマネージャ型２、ＭＲＡＲ型２（３１２）またはＡＣＬマネージャ型３、ＭＲＡＲ型３（３１４）に対応する。ＤＣＥマネージャ型３１０、３１２、３１４は、以下のＤＣＥ　ＡＰＩ
sec_acl_mgr_types_semantics
によって検索することができ、これが、所与のオブジェクトを保護するＡＣＬに対応するマネージャ型のセットを戻す。そして、認可検査の過程で、メソッドのＭＲＡＲの意味規則に対応するＤＣＥ　ＡＣＬが適用される。メソッドのＭＲＡＲをビットマップ列にマッピングすることにより、速やかな認可検査が実行される。

【００２８】二つのアクセス意味規則を区別することができる。

【００２９】１．認可検査がうまく行くためには全ＭＲＡＲセットのＡＮＤ条件が満たされなければならない。これは、全ＭＲＡＲビットマップを、以下のＤＣＥ認可ＡＰＩ
sec_acl_test_access_on_behalf
のための所望のアクセスとしてセットすることに対応する。

【００３０】２．ＭＲＡＲセットの一つの権利だけというＯＲ条件が満たされる必要が出る。この場合、ビットマップ所望アクセス・フラグが一度に１ビットをとり、判定に遭遇するまでＭＲＡＲセットをスパンする。そして、アクセスに失敗すると、全ＭＲＡＲセットをスパンしなければならないが、第一のＭＲＡＲ許可がアクセスを許可すると、認可ルーチンが正常な認可の結果を戻す。

【００３１】まとめとして、本発明の構成に関して以下の事項を開示する。

（１）第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするステップと、メソッド要求アクセス権のセットを割り当てるステップと、前記アクセス権のセットを選択するステップと、を含むことを特徴とする、情報取り扱いシステムにおいてオブジェクト指向技術を用いる方法。

（２）前記方法かステップが、前記アクセス権のセットの二つの要素を検査するステップをさらに含む上記（１）記載の方法。

（３）前記二つの要素の第一のものがファミリー権利型である上記（１）記載の方法。

（４）前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである上記（１）記載の方法。

（５）ファミリー権利型が、オペレーション権利と、役割権利と、を含む上記（３）記載の方法。

（６）第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、メソッド要求アクセス権のセットを割り当てるための手段と、前記アクセス権のセットを選択するための手段と、をさらに含むコンピュータ読み出し可能媒体。

（７）前記媒体が、前記アクセス権のセットの二つの要素を検査するための手段をさらに含む上記（６）記載のコンピュータ読み出し可能媒体。

（８）前記二つの要素の第一のものがファミリー権利型であり、前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである上記（５）記載のコンピュータ読み出し可能媒体。

（９）１個以上のプロセッサと、記憶装置と、ディスプレイ装置を制御するディスプレイ・サブシステムと、カーソル制御装置と、１個以上のＩ／Ｏ装置を制御する１個以上のＩ／Ｏ制御装置と、前記プロセッサ、前記記憶装置、前記ディスプレイ・サブシステム、前記カーソル制御装置および前記Ｉ／Ｏ制御装置を接続するシステム・バスと、システムの動作を制御するためのオペレーテ

ィング・システム・プログラムと、ユーザ・タスクを実行するための一つ以上のアプリケーション・プログラムと、オブジェクト指向制御プログラムと、を含み、前記オブジェクト指向制御プログラムが、第一のクラスによって定義されるメソッドのセットを第一のアクセス権のセットに対してマッピングするための手段と、メソッド要求アクセス権のセットを割り当てるための手段と、前記アクセス権のセットを選択するための手段と、を含むことを特徴とする、分散コンピューティング環境においてオブジェクト・セキュリティ・サービス認可を統合するための情報取り扱いシステム。

（１０）前記アクセス権のセットの二つの要素を検査するための手段をさらに含む上記（９）記載の情報取り扱いシステム。

（１１）前記二つの要素の第一のものがファミリー権利型である上記（１０）記載の情報取り扱いシステム。

（１２）前記二つの要素の第二のものが、ファミリー権利型に関する許可のセットである上記（１０）記載の情報取り扱いシステム。

（１３）前記ファミリー権利型が、関連する許可のセットの意味規則を制御する要素である上記（１１）記載の情報取り扱いシステム。

（１４）ファミリー権利型が、オペレーション権利と、役割権利と、を含む上記（１０）記載の情報取り扱いシステム。

【図面の簡単な説明】

【図１】本発明を具現化するシステムのブロック図である。

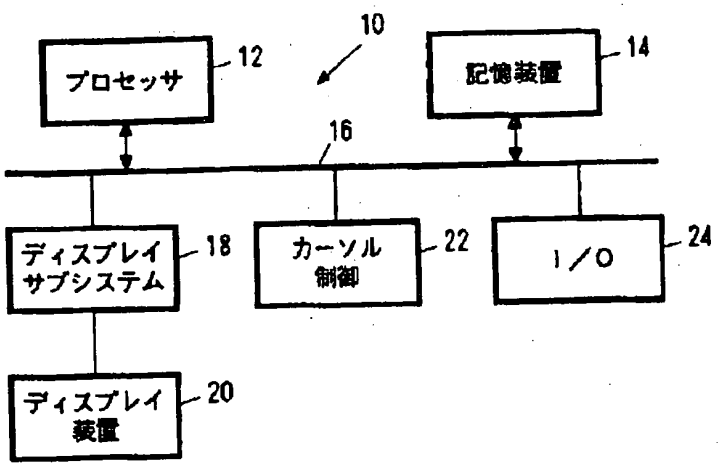
【図２】本発明を支援するオペレーティング・システム・プラットフォームおよびシステム・オブジェクト・モデル・プログラムを示すブロック図である。

【図３】本発明を具現化する分散オブジェクト・システムの略図である。

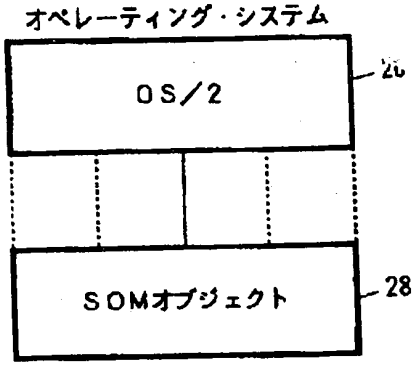
【符号の説明】

１０　情報取り扱いシステム
１２　プロセッサ
１４　記憶装置
１６　システム・バス
１８　ディスプレイ・サブシステム
２０　ディスプレイ装置
２２　カーソル制御装置
２４　Ｉ／Ｏ制御装置
３０２　セキュリティ記憶装置
３０４　システム認可方針オブジェクト
３０６　システム認可オラクル
３０８　ＤＣＥ　ＡＣＬマネージャ
３１０　ＡＣＬマネージャ型１、ＭＲＡＲ型１
３１２　ＡＣＬマネージャ型２、ＭＲＡＲ型２
３１４　ＡＣＬマネージャ型３、ＭＲＡＲ型３

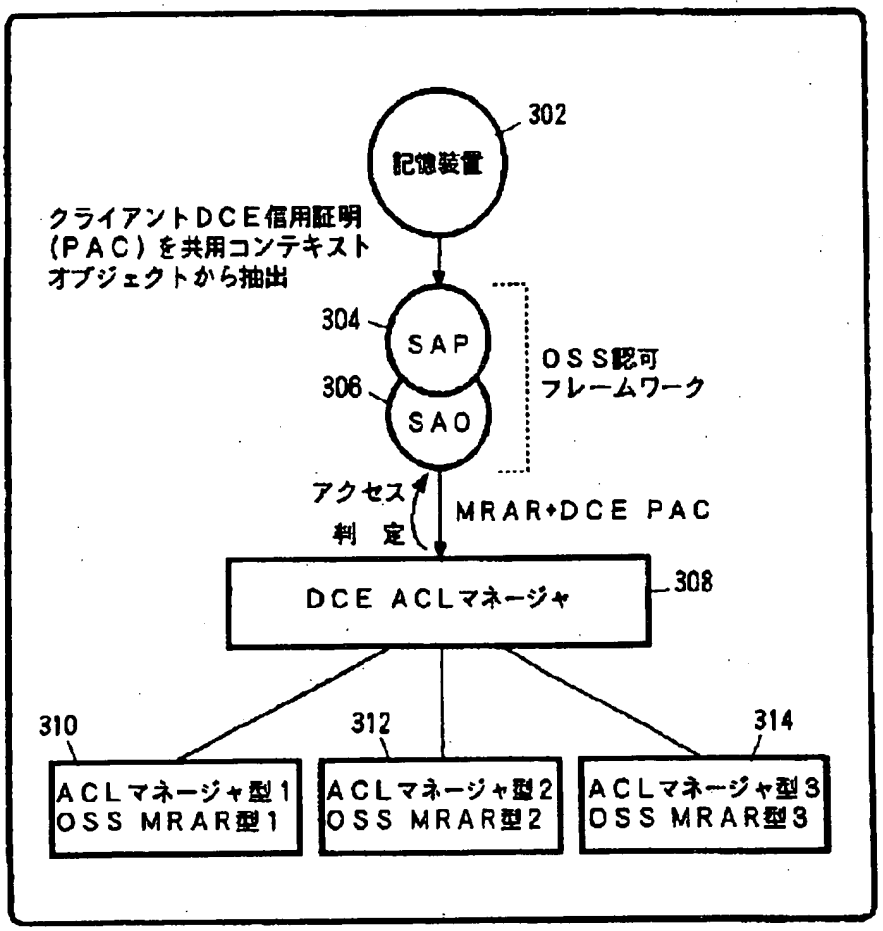
【図１】



【図２】



【図3】



フロントページの続き

(72)発明者　ジョージ・ロバート・ブラクリィ・サード
アメリカ合衆国78729、　テキサス州オースティン　スティルフォレスト　13007

(72)発明者　アンソニー・ジョセフ・ナダリン
アメリカ合衆国78759、　テキサス州オースティン　デュヴァル・ロード　3201　アパートメント　623